DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration
Docket Nos. TSA-2004-19166 and TSA-2004-17982
Notice to Alter Two Existing Systems of Records; Request for Comments

---

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on November 8, 2005, the Department of Homeland Security Transportation Security Administration ("TSA") announced alterations to two existing systems of records and requested comments.[1] According to the notice, TSA is amending the "Categories of individuals covered by the system" portion of the Registered Traveler Operations Files system of records to add a new category:

> Known or suspected terrorists identified in the Terrorist Screening Database (TSDB) of the Terrorist Screening Center (TSC); individuals identified by TSA who are on the Selectee List because they pose a viable threat to civil aviation or national security; and individuals on classified and unclassified governmental terrorist, law enforcement, immigration, or intelligence databases, including databases maintained by the Department of Defense, National Counterterrorism Center, or Federal Bureau of Investigation.[2]

Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the expansion of the Registered Traveler Operations Files system of records ("Registered Traveler"). The watch lists and databases upon which Registered Traveler depends have made thousands of false matches, and problems associated with them are exacerbated by fact that the databases are not subject to the full safeguards of the Privacy Act of 1974, 5 U.S.C. § 552(a). Additionally, though the TSA pilot phase of Registered Traveler

---

[1] Notice to Alter Two Existing Systems of Records; Request for Comments, 70 Fed. Reg. 67731 (Nov. 8, 2005).
[2] *Id*. at 67732.

concluded on October 11, 2005, Transportation Security Administration Director Kip Hawley also has testified that Registered Traveler will launch again on June 20, 2006.[3] TSA also is continuing to conduct background checks for a Registered Traveler program named Clear, operated by Verified Identity Pass Inc.[4] This private company is not subject to the Privacy Act.[5]

Given these problems, EPIC urges the Transportation Security Administration to suspend the private Registered Traveler program Clear (and any private programs) until it can address the serious privacy implications involved in the use of watch lists and databases. EPIC also urges suspension of the program until the agency crafts regulations to ensure that the information collection and maintenance practices of Verified Identity Pass (or any other private company operating a Registered Traveler program) comply fully with the intent of the Privacy Act.

Introduction

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[6] The Supreme Court just last year underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to

[3] Leslie Miller, *U.S. Plans "Registered Traveler" Program,* Associated Press, Nov. 3, 2005.
[4] Thomas Frank, *Biometric IDs could see massive growth*, USA Today, Aug. 15, 2005.
[5] 5 U.S.C. § 552(a).
[6] S. Rep. No. 93-1183 at 1 (1974).

> individuals aggrieved by failures on the Government's part to comply with the requirements.[7]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[8] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[9] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[10]

Among the key provisions of the Privacy Act is the opportunity to inspect and correct records held by federal agencies. 5 U.S.C. 552(a)(d) ensures that records are accurate and reliable. However, under the Privacy Act regulations proposed by TSA for Registered Traveler, individuals have no such right and therefore the likelihood of errors is increased.[11]

Adherence to these requirements is critical for a massive repository like Registered Traveler. Information in the system includes some, or all, of the following:

> (a) Full name.
> (b) Current home address.
> (c) Current home phone number.
> (d) Current cell phone number (if applicable).
> (e) Social security number.
> (f) Date of birth.
> (g) Place of birth.

---

[7] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[8] S. Rep. No. 93-1183 at 1.
[9] Pub. L. No. 93-579 (1974).
[10] *Id*.
[11] 70 Fed. Reg. at 67736.

(h) Nationality.
(i) Gender.
(j) Prior home addresses.
(k) Arrival date in United States (non-U.S. citizens only).
(l) Digital photo.
(m) Reference biometric (i.e. fingerprint(s), iris scan, facial geometry, hand geometry, handwriting/signature, others).
(n) Unique identification record number.
(o) Unique token or credential serial number.
(p) Security assessments.
(q) Information pertaining to adjudication results.
(r) RT eligibility status.
(s) Token or credential issue date.
(t) Token or credential expiration date.
(u) Information and data provided by Federal, State, and local government agencies and foreign governments that is necessary to conduct a security assessment to determine if an individual poses a potential threat to aviation security.
(v) Authorized Federal LEOs may have a Federal LEO code name and unique administrative code number.[12]

EPIC has previously submitted comments about the Registered Traveler system, highlighting the privacy problems and urging the agency not to claim exemptions from the Privacy Act unless necessary and justifiable.[13] These problems maybe all the more injurious to air travelers if the program is run by private company not subject to any Privacy Act safeguards. Therefore, EPIC urges the Transportation Security Administration to address the security and privacy implications in the Registered Traveler program.

I. TSA Has Admitted Mistakenly Matching Thousands of Innocent People To Its Watch Lists

TSA seeks to expand the number of individuals covered by the Registered Traveler system, including those "individuals identified by TSA who are on the Selectee

[12] 70 Fed. Reg. at 67735.
[13] Comments of the Electronic Privacy Information Center, Docket No. TSA-2004-17982 (July 1, 2004), *available at* http://www.epic.org/privacy/airtravel/rt_comments.pdf.

List because they pose a viable threat to civil aviation or national security."[14] However, the "selectee" and "no-fly watch lists" have led to thousands of erroneous matches. Earlier this week, Jim Kennedy, director of the Transportation Security Administration's redress office, admitted that about 30,000 airline passengers were mistakenly matched with names appearing on TSA's "selectee" watch list.[15]

It is well known that individuals encounter difficulty in resolving problems associated with being improperly flagged by watch lists. Documents obtained earlier this year by EPIC under the Freedom of Information Act show travelers struggle to clear their names.[16] One person named in the documents, Sister Glenn Anne McPhee, the U.S. Conference of Catholic Bishops' secretary for education, spent nine months attempting to clear her name from a TSA watch list. The process was so difficult, Sister McPhee told a reporter, "Those nine months were the closest thing to hell I hope I will ever experience."[17]

Senators Ted Kennedy (D-MA) and Don Young (R-AK) also have been improperly flagged by watch lists.[18] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge. Unfortunately, most people do not have that option.

---

[14] 70 Fed. Reg. at 67732.
[15] Anne Broache, *Tens of thousands mistakenly matched to terrorist watch lists*, CNet News, Dec. 6, 2005.
[16] EPIC FOIA Notes, *Travelers Continue to Struggle with Watch List Errors*, No. 8 (Sept. 27, 2005), *available at* http://www.epic.org/foia_notes/note8.html.
[17] Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005.
[18] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Washington Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press International, Aug. 20, 2004.

In March, Rep. Loretta Sanchez (D-CA) expressed dismay to TSA officials that current TSA safeguards had failed her constituents. At a House subcommittee hearing on March 2, 2005, Rep. Sanchez reported that many of her constituents continue to face lengthy delays, questioning, and at times are prohibited from boarding flights because they are misidentified as people sought on watch lists. Her constituents continue to face these roadblocks even after they apply for, receive and then display to screener personnel the official federal government letters that establish their innocence. Rep. Sanchez questioned why current redress procedures have failed these American citizens.[19]

These problems are also a part of the private Registered Traveler program run by Verified Identity Pass, called "Clear." "Although Verified ID claims that members of the program will be provided with the identification information in the private database, the most pertinent information will not be revealed to those people who provide information to the Registered Traveler system," EPIC Executive Director Marc Rotenberg testified before Congress last month.[20] He explained:

> For instance, if an applicant is denied membership, or if a member's status on the watch lists changes, the individual is never told why he has been deemed a potential security risk. Furthermore, applicants who have supplied sensitive personal information to the program are not assured of access to the information that the system has on them, and therefore have no way of ensuring either the accuracy or the security of their data.[21]

[19] Shaun Waterman, *No Redress Mechanism in New DHS Terrorist Screening Office,* United Press International, Mar. 2, 2005.
[20] Marc Rotenberg, Executive Director, EPIC, *Prepared Testimony and Statement for the Record*, Hearing on "The Future of Registered Traveler" Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, U.S. House of Representatives Committee on Homeland Security (Nov. 3, 2005), *available at* http://www.epic.org/privacy/airtravel/rt_test_110305.pdf.
[21] *Id*. at 2, 3.

The difficulties that innocent air travelers have had made clear that TSA should suspend the private Registered Traveler program "Clear" and any other Registered Traveler programs until the significant privacy implications of the use of watch lists are resolved.

II. TSA Must Subject Private Companies Operating Registered Traveler Programs To Privacy Act Restrictions

As previously noted, Congress adopted the Privacy Act of 1974 after extensive hearings and careful consideration. The Act requires government agencies to limit the collection, sharing, and use of individuals' personal information, and that agencies give individuals the right to access and correct information the government collects about them.[22] In the next few months, private security companies will introducing Registered Traveler programs at as many as 40 of the largest domestic airports, according to Steven Brill, who runs Clear parent company Verified Identity Pass.[23]

Executive Director Rotenberg noted in his November Congressional testimony that:

> In the case of a private partner, the data collected from passengers is stored in a separate, private database. As a private entity, the partner is not covered by any of the requirements of the Privacy Act. When TSA says that its contractors must abide by the Privacy Act, this is only with regard to the information flowing from the TSA to the contractor, not for this separate, private database of personal information collected and kept by the private company. Thus, the only guarantee of privacy that passengers have comes from the company's own broad assurances.[24]

This creates a risk of "mission creep," where the sensitive passenger information collected by private companies could be used in ways not originally intended. Clear program applicants must submit a substantial amount of personally identifiable

[22] 5 U.S.C. § 552(a).
[23] Joe Sharkey, *Green Light for Security Card*, New York Times, Nov. 5, 2005.
[24] Rotenberg Testimony at 3.

information that Clear keeps – including biometric data and digital images of identity documents, such as birth certificates, Social Security cards, and driver's licenses. It is possible for program members to be tracked, because the company "will maintain 'log files' of entrances to local venues."[25] The company states that it keeps the log files only at the local venue and these files are automatically purged every 24-48 hours.[26] However, the possibility for easily tracking travelers is there, and it would be tempting do so.

Privacy and security concerns also arise from comments made by Clear CEO Steven Brill. Mr. Brill has said that he envisions the Clear card becoming more than just an aviation security ID card. Mr. Brill's company has partnered with rental car company Hertz and online travel booking company Orbitz to market the Clear program cards, and is expected to partner with an airline.[27] Mr. Brill has said that he hopes the Clear ID card would also be used at office buildings, power plants and stadium.[28] This would be a significant and troubling expansion of the Registered Traveler program and further undermine the interests the Privacy Act seeks to protect.

Conclusion

About 30,000 air passengers have reported being wrongly matched to the TSA watch lists. This has caused significant frustrations, from long delays to the inability to board planes. These problems flow from the failure to fully apply Privacy Act safeguards, particularly 5 U.S.C. 552(a)(d), which would provide a right of access and correction to individuals. Moreover, the administration of the program by a private contractor, not subject to any Privacy Act obligations would lead to even more problems. EPIC therefore

[25] Clear Registered Traveler *at* http://flyclear.com/.
[26] *Id*.
[27] Laura Meckler, *Air Security: Shorter Waits For More Fliers?,* Wall Street Journal, Sept. 28, 2005.
[28] Brian Bergstein, *Voluntary Security ID to Debut in Florida*, Associated Press, June 3, 2005.

urges the Transportation Security Administration to suspend all Registered Traveler programs until private companies administering them are made subject to the legal safeguards of the Privacy Act of 1974 and until the privacy and security problems associated with the watch lists can be resolved.

Respectfully submitted,

_____

Marc Rotenberg
Executive Director

_____

Melissa Ngo
Staff Counsel